Contents

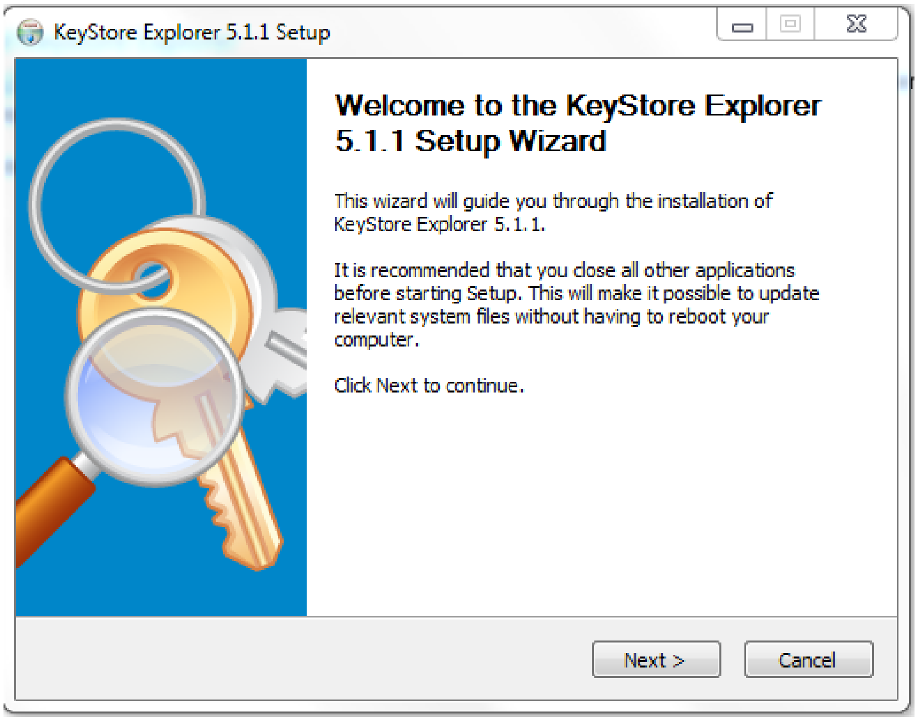
Creating a JAVA Keystore

Download and Install Keystore Explorer

Go to http://keystore-explorer.sourceforge.net/downloads.php and then download the latest version of keystore explorer software suiting your OS.

Install the downloaded executable following the normal standard procedure.

Step 1: Click on Next.



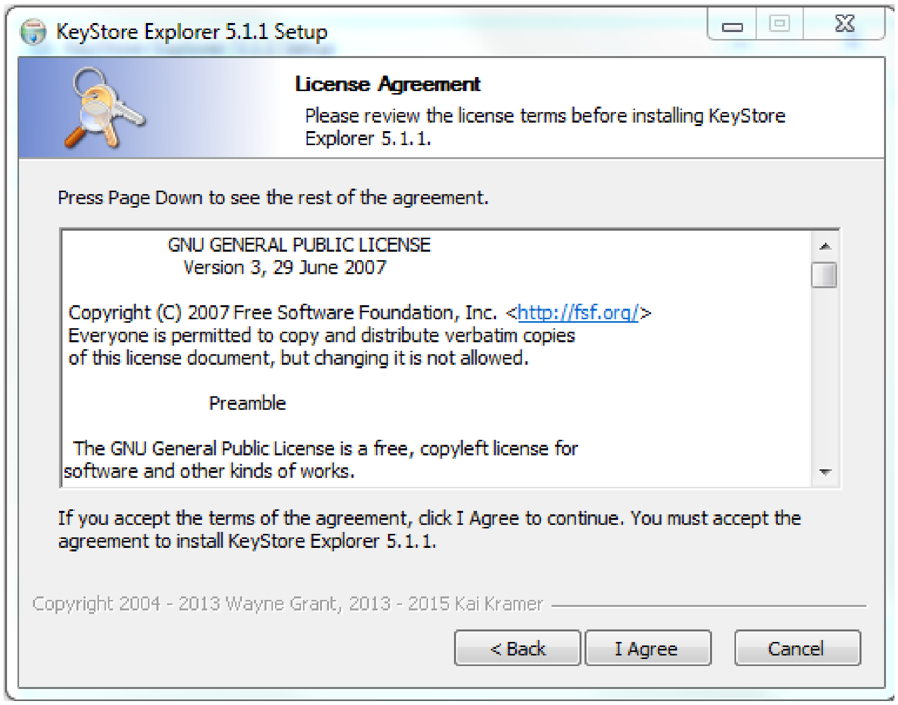
Welcome to the KeyStore Explorer 5.1.1 Setup Wizard

This wizard will guide you through the installation of KeyStore Explorer 5.1.1.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Step 2: Click on I Agree.



License Agreement

Please review the license terms before installing KeyStore Explorer 5.1.1.

Press Page Down to see the rest of the agreement.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

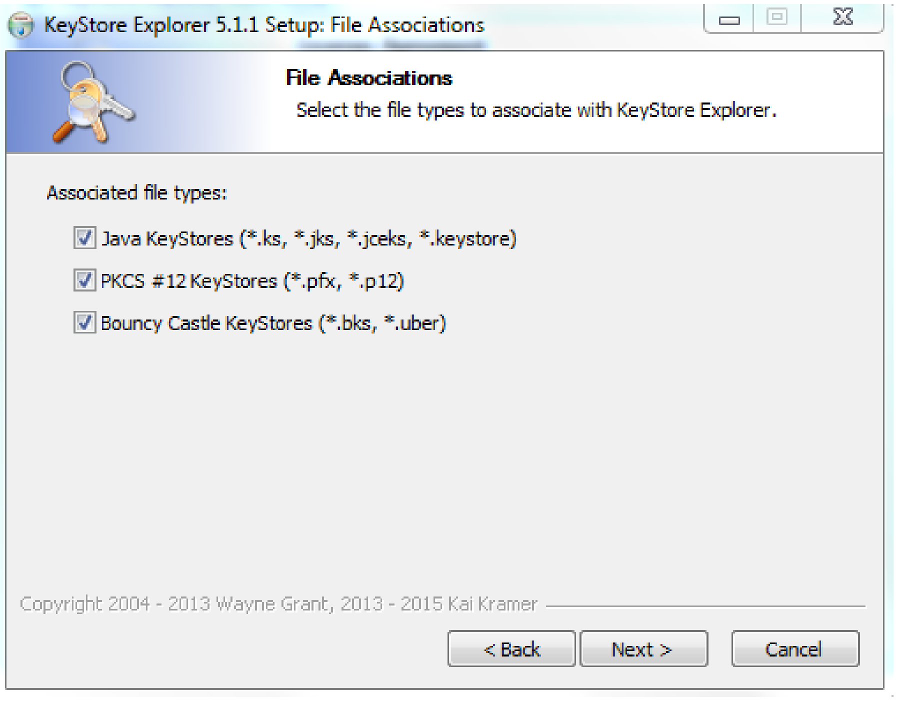
Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install KeyStore Explorer 5.1.1.

Copyright 2004 - 2013 Wayne Grant, 2013 - 2015 Kai Kramer

Step 3: Click on Next



File Associations

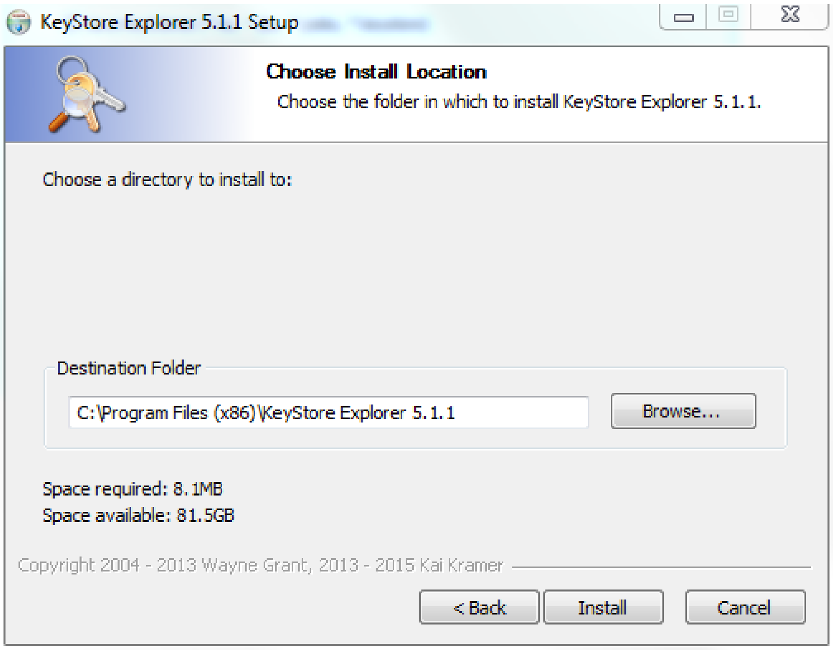
Select the file types to associate with KeyStore Explorer.

Associated file types:

- ☑ Java KeyStores (*.ks, *.jks, *.jceks, *.keystore)
- ☑ PKCS #12 KeyStores (*.pfx, *.p12)
- ☑ Bouncy Castle KeyStores (*.bks, *.uber)

Copyright 2004 - 2013 Wayne Grant, 2013 - 2015 Kai Kramer

Step 4: Click on Install wait for the installation to complete.



KeyStore Explorer 5.1.1 Setup

Choose Install Location

Choose the folder in which to install KeyStore Explorer 5.1.1.

Choose a directory to install to:

Destination Folder: C:\Program Files (x86)\KeyStore Explorer 5.1.1

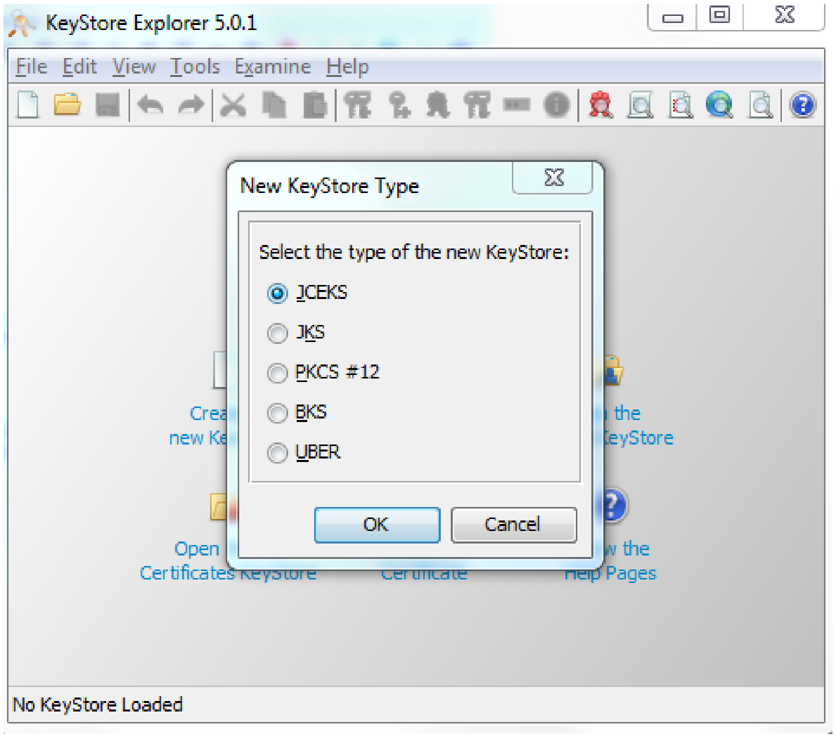
Space required: 8.1MB
Space available: 81.5GB

Copyright 2004 - 2013 Wayne Grant, 2013 - 2015 Kai Kramer

Creating a Keystore

Once the installation is complete, open the keystore explorer application.

Then click on 'Create a new Keystore' for creating a keystore. Select 'JCEKS' for type of keystore.



KeyStore Explorer 5.0.1

New KeyStore Type

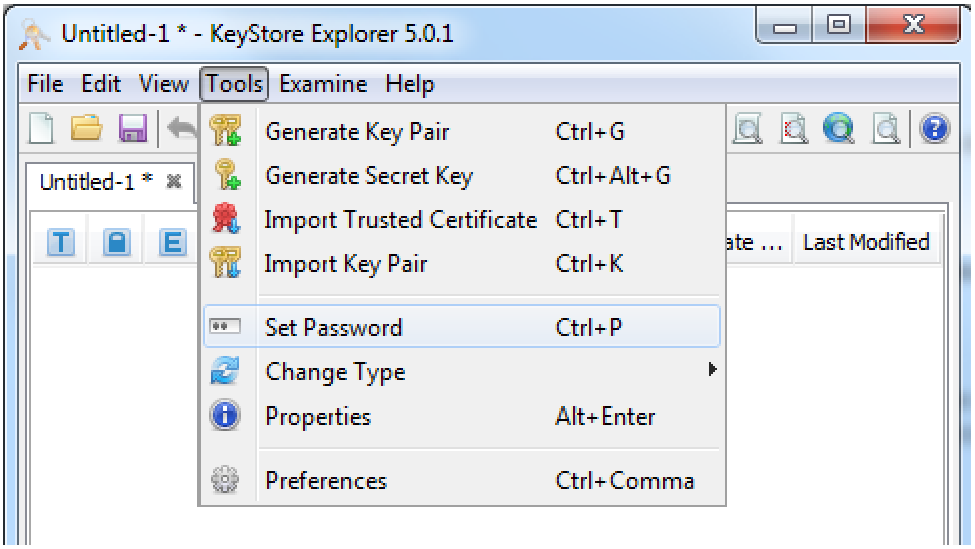
Select the type of the new KeyStore:

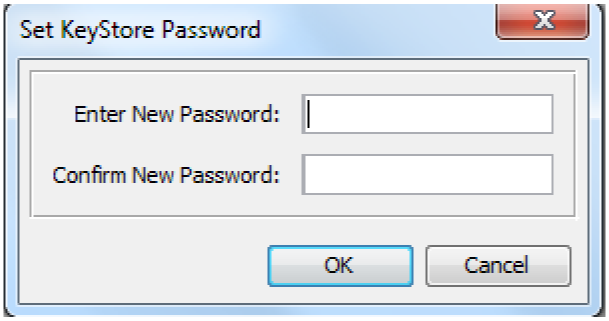
- ● JCEKS
- ○ JKS
- ○ PKCS #12
- ○ BKS
- ○ UBER

No KeyStore Loaded

Click on Tools -> Set Password to set a password for the keystore.

NOTE: Remember this password as it cannot be retrieved if forgotten. Also the keystore will not be usable without this password.

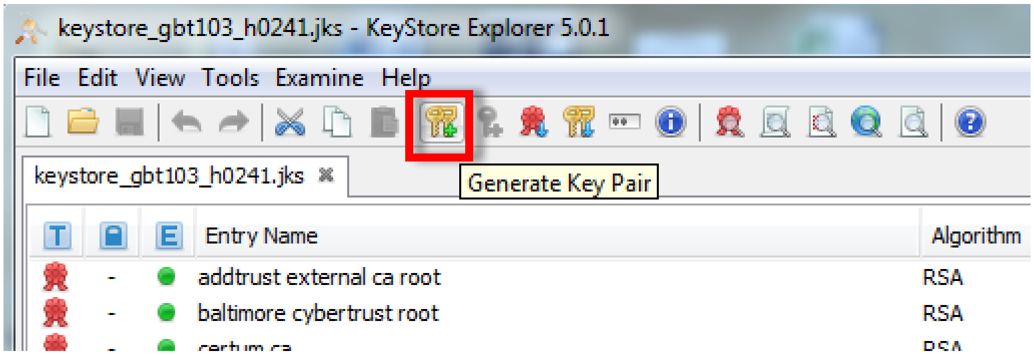




Key Pair Generation

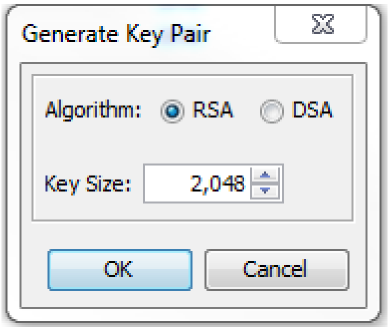
Once the password is set, generate the Key pair using the following steps.

Step 1: Click on 'Generate Key Pair' Option


keystore_gbt103_h0241.jks - KeyStore Explorer 5.0.1
File Edit View Tools Examine Help
keystore_gbt103_h0241.jks
Generate Key Pair
Entry Name
Algorithm

T	🔒	E	Entry Name	Algorithm
	-	●	addtrust external ca root	RSA
	-	●	baltimore cybertrust root	RSA
	-	●	certum ca	RSA

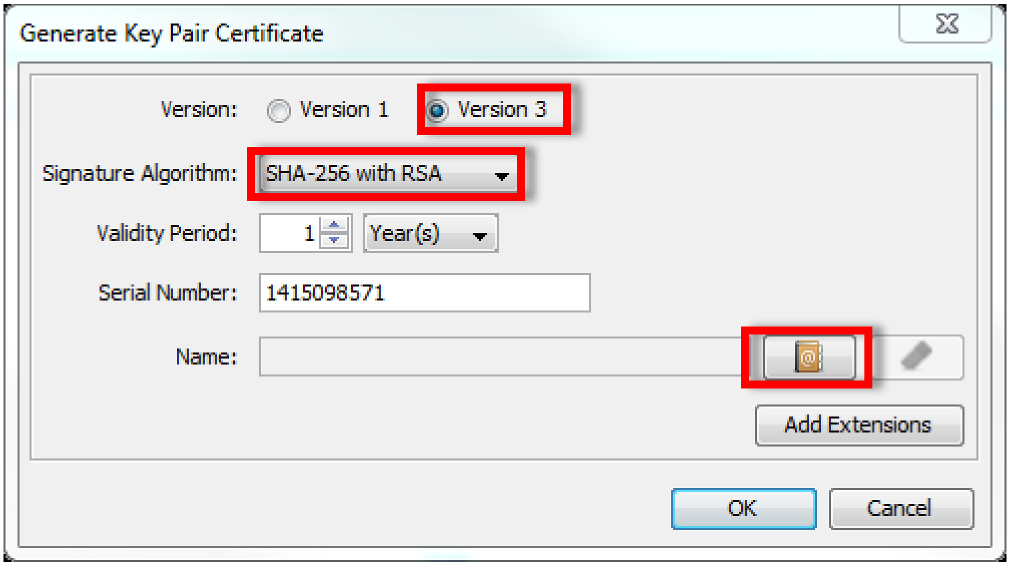
Step 2: Select the RSA algorithm and key size 2048


Generate Key Pair

Algorithm: ● RSA ○ DSA

Key Size: 2,048

Step 3: Select Version 3, SHA-256 with RSA and select the icon as below.


Generate Key Pair Certificate

Version: ○ Version 1 ● Version 3

Signature Algorithm: SHA-256 with RSA

Validity Period: 1 Year(s)

Serial Number: 1415098571

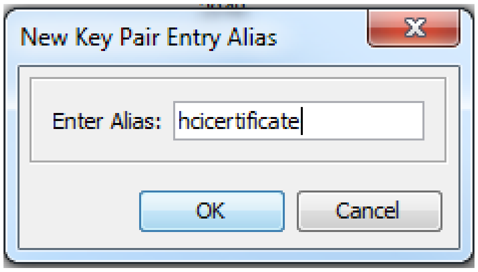
Name:

Step 4: Enter all the required details

Common Name (CN):	Worker Node URL
Organization Unit (OU):	<Small organization name of your company>
Organization Name (O):	<Large organization name of your company>
Locality Name (L):	<Locality of your company>
State Name (ST):	<State Name>
Country (C):	<Country Code>

Note: Worker Node URL can be fetched from the customer release mail. Please remove ‘https://’ and enter the rest of the URL in ‘Common Name (CN) :’ field.

Step 5: Enter Alias name as hcicertificate



Enter Alias: hcicertificate

Step 6: Set the password for the Key pair. Enter the same password supplied for the keystore password.

Note: Key pair password and Keystore password should be the same.

With these steps, key pair generation is complete.

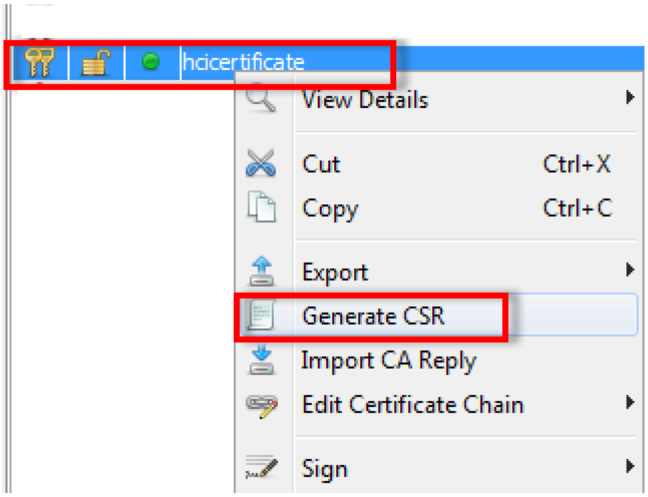
CSR Generation

CSR (Certificate Signing Request) is required for signing the key generated. Only the signed certificate needs to be used for the SSL communication from the HCI tenant to the end systems.

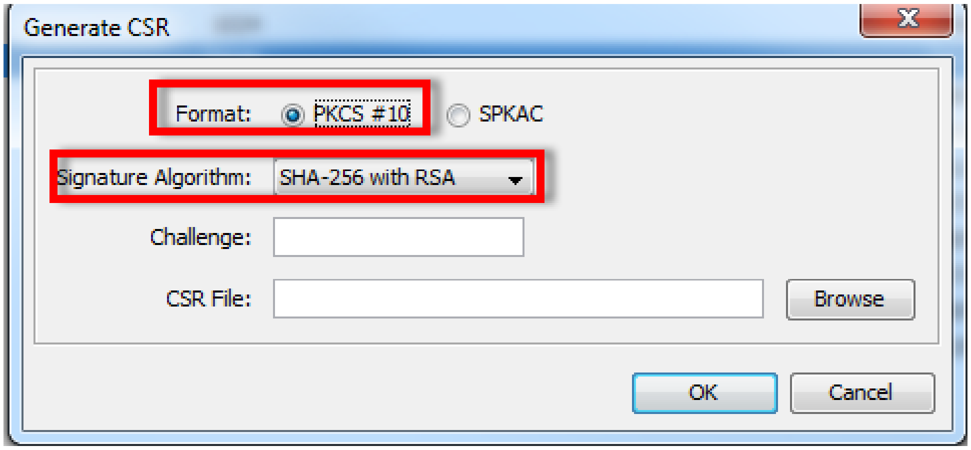
The current list of Certifying Authorities (CAs) approved by HCI can be found in https://proddps.hana.ondemand.com/dps/d/preview/93810d568bee49c6b3d7b5065a30b0ff/2015.03/en-US/frameset.html?4509f605e83c4c939a91b81eb3a6cdea.html . These are the list of CAs which can be used for signing the CSR.

Use the below steps to generate a CSR.

Step 1: Right click the Key pair and select Generate CSR



Step 2: Select right format and algorithm.



Format: ● PKCS #10 ○ SPKAC

Signature Algorithm: SHA-256 with RSA

Challenge:

CSR File:

Step 3: Store the file name as <FILENAME>.csr

Uploading CSR for Signing

Every CA have a unique way to perform this action and hence it would be better to check with the respective CA's home page for more information on how to do this.

Importing Signed certification into keystore

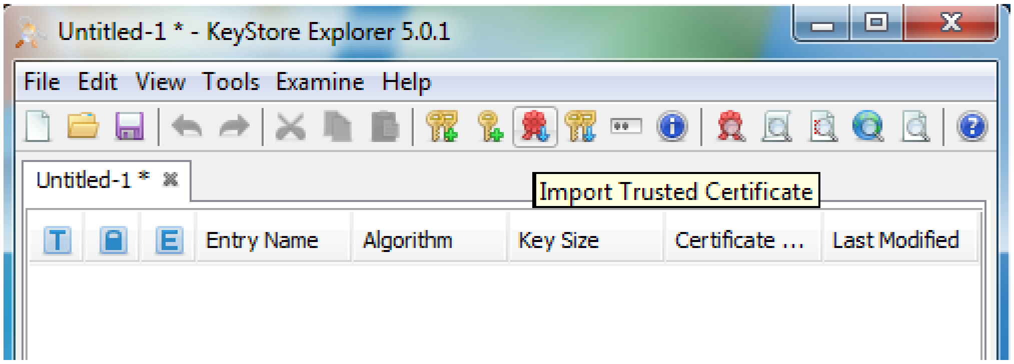
Once the CSR is uploaded into the CA's website for signing, the signed certificate reply will be sent back to the requestor by the CA via mail or other means of communication.

Importing Trusted Certificates

Before importing this signed certificate response into the keystore, the root and intermediate of the CA needs to be imported into the keystore. Follow the below steps to perform the same.

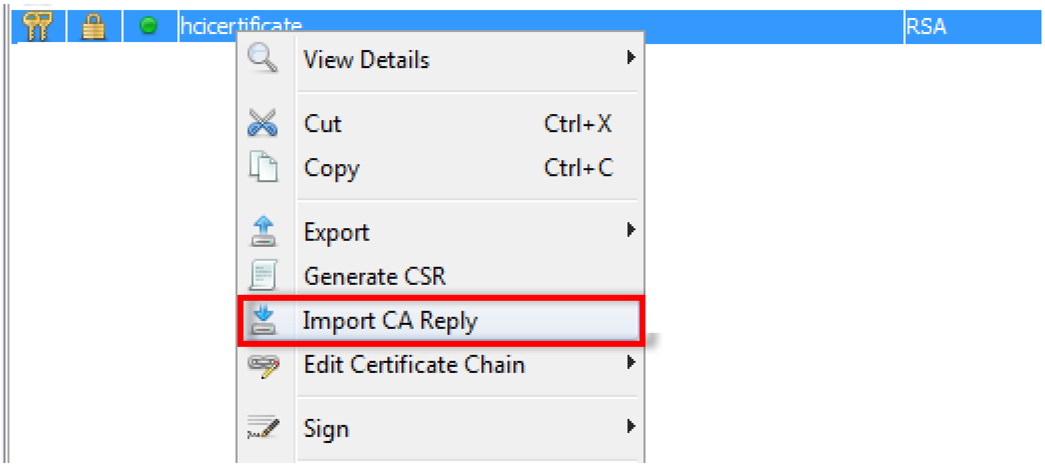
Step 1: Download the root and intermediate CAs from the certifying authorities (CAs) website. Save those files in .cer or .crt format.

Step 2: Click on 'Import Trusted Certificates' Icon, Select the files downloaded and then click on 'Import'.

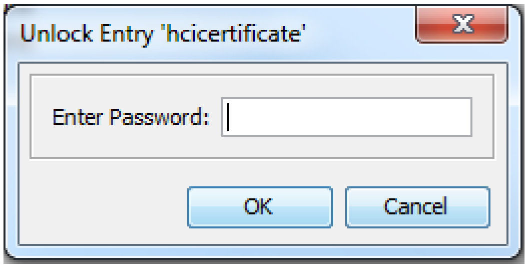


Import CA Reply

Step 1: Right click the Key pair (hcicertificate) and select Import CA Reply from the context menu



Step 2: Enter the Key pair password and select OK.



Step 3: Select the relevant .crt file and import the CA reply.